

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Records and information associated with the cellular
device assigned 414-418-8150 that is stored at premises
controlled by AT&T

Case No. 20m811

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 241

The application is based on these facts: See attached affidavit.

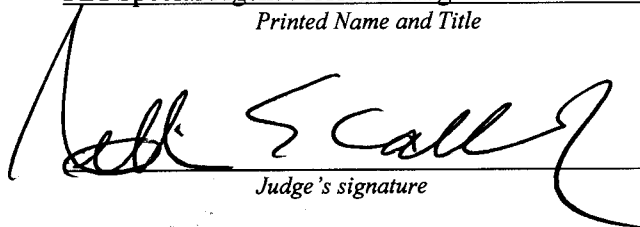
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

FBI Special Agent Jessica Krueger
Printed Name and Title

Sworn to before me and signed in my presence:

Date: January 9, 2020


Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Callahan, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jessica Krueger, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephone assigned call number 414-418-8150, (the "Target Cell Phone"), whose service provider is AT&T, ("Service Provider") a wireless telephone service provider with its global legal demand center headquartered in North Palm Beach, FL. The Target Cell Phone is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. I am a Special Agent with the FBI and have been since November 2009. I am involved in investigations of persons suspected of violations of Federal law in the State of Wisconsin and throughout the United States. I am currently assigned to the Milwaukee Field Office, where I conduct a variety of investigations in the area of counterterrorism, including domestic and international terrorism. I have investigated and assisted in the investigation of matters that involve the use of computers, telephones, encrypted messaging platforms and other electronic devices in furtherance of criminal activity.

3. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information obtained from

other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 241 (conspiracy against rights) have been committed by Yousef Omar Barasneh. There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and will lead to the identification of individuals who are engaged in the commission of these offenses.

5. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. The FBI is investigating criminal activity by members of an organization called “The Base,” a neo-Nazi group that aims to unify militant white supremacists around the globe and provide them with paramilitary training in preparation for a “race war.” As described herein, one or more individuals associated with “The Base” are suspected of vandalizing a synagogue in Racine, Wisconsin, in September 2019, in violation of, among other things, 18 U.S.C. § 241, which makes it a felony to “conspire to injure, oppress, threaten, or intimidate any person in any State, Territory, Commonwealth, Possession, or District in the free

exercise or enjoyment of any right or privilege secured to him by the Constitution or laws of the United States.” As part of the investigation, agents have identified the Target Cell Phone number as being associated with an individual believed to be involved in the Racine synagogue attack.

7. On September 22, 2019, law enforcement officers in Wisconsin discovered that the Beth Israel Sinai Congregation located at 3009 Washington Avenue Racine, Wisconsin had been vandalized. Specifically, the officers saw swastikas, the symbol for The Base, and anti-Semitic words spray-painted on the exterior of the building. The synagogue is an active organization comprised of Jewish members who worshiped and conducted other religious activities therein.

8. Similarly, on September 21, 2019, law enforcement officers in Hancock, Michigan discovered that the Temple Jacob had been vandalized. Specifically, they saw swastikas and the symbol of The Base spray-painted on the exterior of the building. As with the synagogue in Racine, Wisconsin, the synagogue in Michigan is an active organization comprised of Jewish members who worshiped and conducted other religious activities therein.

9. Based on my training and experience and familiarity with this investigation, I am aware that The Base is a white racially motivated extremist group that describes itself as a “international survivalism & self-defense network, for nationalist of European descent,” and offers “IRL” (in real life) survivalist training to resist “our People's extinction,” or the extinction of the white race. Members of The Base communicate with each other through online platforms and

encrypted online messaging applications and chat rooms. In these communications, they have discussed, among other things, acts of violence against minorities (including African Americans and Jewish-Americans), Base military training camps, and ways to make improvised explosive devices ("IEDs"). The symbol used by The Base is a black flag with three white Runic Eihwaz symbols.

10. Based on information I have received during the course of this investigation, I am aware that The Base has been active in Wisconsin and that there are members of the "North Central region," alternatively known as the "Great Lakes cell," based in Wisconsin. For instance, in early June 2019, Base recruitment flyers were posted at Marquette University in Milwaukee, WI. In July 2019, The Base organized an armed training session for members in Wood County, Wisconsin, and posted photos to social media about the session. And, as noted above, the symbol for The Base was discovered spray-painted on the Beth Israel Sinai Congregation synagogue in Racine, WI.

11. As part of the investigation, the FBI received information from an individual associated with The Base, who I will refer to as co-conspirator #1 ("CC1"). In statements to the FBI between October 2019 and December 2019, CC1 admitted that in September 2019, he directed other members of The Base to vandalize minority-owned properties throughout the country. CC1 called this "Operation Kristallnacht"¹ and directed others to "tag the shit" out of synagogues. Based on my

¹ Based on publicly available information, I am aware that Operation Kristallnacht, or the Night of Broken Glass, is an event that occurred in Nazi Germany on November 9 and 10, 1938. During this

training and experience and familiarity with this investigation, I believe that CC1 meant that synagogues should be spray-painted with anti-Semitic graffiti. Further, based on my training and experience and familiarity with this investigation, I believe that a goal of such action is to intimidate and threaten Jewish citizens who use the synagogue for worship and other religious activities. CC1 further elaborated on his instructions to other Base members, stating that "if there's a window that wants to be broken, don't be shy." CC1 told the FBI that the operation was nationwide, and that CC1 knew members of The Base's Great Lakes cell carried out attacks against synagogues in Wisconsin and Michigan.

12. CC1 stated that the person who carried the attack on the synagogue in Racine, Wisconsin, was a Base member known as "Joseph" or "Josef." CC1 stated that Joseph was a member of The Base's Great Lakes cell and was from Wisconsin. According to CC1, after the Racine synagogue attack, Joseph sent CC1 a message on an encrypted platform with a news article about the attack and wrote something to the effect of "here's what I did."

13. CC1 stated that CC1 had never met Joseph in person. But, they had communicated with each other via encrypted messages, and CC1 knew Joseph to be a large individual as Joseph's large size was a common joke in The Base chat rooms.

time, Jewish homes, hospitals, and schools throughout Germany were ransacked and demolished by Nazi paramilitary soldiers and civilians. The name "Kristallnacht" comes from the shards of broken glass that littered the streets after the windows of Jewish-owned stores, buildings, and synagogues were smashed.

CC1 and Joseph had planned to meet in person at a Base meeting in Georgia in late October/early November 2019, but CC1 ultimately did not attend that meeting.

14. Information provided by CC1 has been corroborated by investigators. For instance, in November 2019, the FBI obtained a search warrant for CC1's residence and electronic devices. In CC1's electronic devices, investigators found evidence showing that that around September 17, 2019 and again on September 21, 2019, CC1 conducted multiple Google searches for "Kristallnacht." Following the search for "Kristallnacht" on September 17, 2019, CCI used an internet browser to access an encrypted messaging application known to be utilized by members of The Base. The digital evidence showed that CCI accessed the encrypted messaging application and visited a section of the application that was labeled with the symbol for The Base.

15. On September 23, 2019, CC1 conducted multiple Google searches for "racine, wi," "racine wi nazi," and "racine wi anti-semitic." CCI also accessed news websites and Twitter that had posted articles and comments on the Racine synagogue vandalism. Further, the device evidence shows that on September 23, 2019, CC1 accessed the same encrypted messaging application noted above. The evidence showed that CCI accessed a section of the encrypted messaging application that was labeled with "JOSEPH." Based on my training and experience and my involvement in this investigation, I believe that CC1 was using the encrypted messaging application to exchange messages with members of The Base, including "JOSEPH."

16. CC1 has been arrested and charged in another federal district court with violating 18 U.S.C. § 241. The charges relate to CC1's conduct in directing other Base members to attack synagogues in Racine, Wisconsin, and Hancock, Michigan, as described above.

17. As part of the investigation, agents identified several dates and locations where members of the Base were believed to have been. This included (1) July 27, 2019, the date that The Base conducted training at the Wood County Firing Range, 3705 Marsh Road, Town of Seneca, Wood County, WI 54495; and (2) the evening of September 21, 2019, when the Beth Israeli Sinai Congregation located at 3009 Washington Avenue Racine, Wisconsin, was vandalized.

18. Thereafter, pursuant to a court order, agents obtained information about cell phone connections to towers near those locations on those dates. The cell tower information revealed that, on July 27, 2019, between 7:00 a.m. and 7:00 p.m., the Target Cell Phone number pinged approximately 78 times off the tower close to 3705 Marsh Road, Town of Seneca, Wood County, WI 54495. The information further showed that on September 21, 2019, between 8:55 p.m. and 10:08 p.m., the Target Cell Phone number pinged approximately 5 times off the tower close to 3009 Washington Avenue, Racine, Wisconsin.

19. Records show that during the relevant time period, the Target Cell Phone number has been issued by AT&T to subscriber Omar Ali Barasneh and user Yousef Barasneh, with a billing address 1101 E Forest Hill Avenue, Oak Creek, Wisconsin 53154. Police records further show that on October 24, 2017, Yousef

Omar Barasneh, the adult son of Omar Ali Barasneh, had contact with the Oak Creek Police Department and reported to the officers that the Target Cell Phone number was his (Yousef's) phone number. Records from the Wisconsin Department of Motor Vehicles show that Yousef Omar Barasneh was born 11/26/1997, lists 1101 E Forest Hill Avenue, Oak Creek, Wisconsin 53154, as his residence, and that he is 6'2" and 300 lbs.

20. The evidence sought through this applied-for search warrant is relevant for investigators to determine, among other things, the activities of the Target Cell phone user with regard to The Base and synagogue vandalism. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

Cell-Site Data

21. Based on my training and experience, I know that the Service Provider can collect cell-site data on a prospective basis about the Target Cell Phone. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

Subscriber Information

22. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other

communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

23. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

24. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

25. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

Records and information associated with the cellular device assigned 414-418-8150 (referred to herein and in Attachment B as “the Target Cell Phone”), that is in the custody or control of AT&T (referred to herein and in Attachment B as the “Provider”), a wireless communications service provider with its global legal demand center headquartered at 11760 U.S. Highway 1, North Palm Beach, FL.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

- a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period January 1, 2019 through the present:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber

Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

- vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records;
- ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone account, including:
 - (i) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - (ii) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received),

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 241 involving Yousef Omar Barasneh during the period January 1, 2019, through the present.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by AT&T, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of AT&T. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of AT&T, and they were made by AT&T as a regular practice; and

b. such records were generated by AT&T's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of AT&T in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by AT&T, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature